Lattices in Algebraic Coding Theory

Master thesis by Cyril Becker, supervised by Prof. Eva Bayer and Dr. Roope Vehkalahti

Presentation of the problem

A *space-time* code $\mathcal{C}$ is a subset of $M_n(\mathbb{C})$ involving one sender and one receiver. Both the sender and the receiver are equipped with n antennas. If the sender transmits $X \in \mathcal{C}$, the receiver will get

$$Y = HX + V \in M_n(\mathbb{C}), \text{ with } H, V \in M_n(\mathbb{C}).$$

In order for the receiver to uniquely recover the sent codeword, we study codes of the form

$$\mathcal{C} = \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k \subseteq M_n(\mathbb{C}),$$

with $\mathbb{R}$-linearly independent matrices $M_1, \ldots, M_k \in M_n(\mathbb{C})$. We call k the dimension of the code, and we talk about *lattice codes*.
The *minimum determinant* of a code is

$$\min\det(\mathcal{C}) = \inf_{X \in \mathcal{C}, X \neq 0} \{|\det(X)|\}.$$

If the minimum determinant of a code stays above a positive constant, we talk about code having *non-vanishing determinant* (NVD) property. It turns out that maximizing the minimum determinant of a code amounts to improving its efficiency.

However, to be able to compare two codes, we need the notion of *normalized minimum determinant* which is defined hereafter. The following problem is studied in the thesis.

Find the maximal k such that $\mathcal{C} = \mathbb{Z}M_1 \oplus \cdots \oplus \mathbb{Z}M_k \subseteq M_n(\mathbb{C})$, with $\mathbb{R}$-linearly independent matrices $M_1, \ldots, M_k$, has NVD property; and give explicit constructions.

Tools from lattice theory

Let V be an m-dimensional $\mathbb{R}$-vector space. A *lattice* in V is a subgroup of the form

$$L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k \subseteq V,$$

with $\mathbb{R}$-linearly independent vectors $v_1, \ldots, v_k$ of V.
We call *fundamental parallelotope* of L the following set

$$\mathcal{F}_L = \{x_1v_1 + \cdots + x_kv_k : x_i \in \mathbb{R}, 0 \leq x_i < 1\}.$$

Choose an isomorphism $\beta : \mathbb{R}(L) \xrightarrow{\sim} \mathbb{R}^k$. The *volume* of L denoted by $\mathrm{vol}(L)$ may be defined to be the Lebesgue measure of $\beta(\mathcal{F}_L)$ in $\mathbb{R}^k$.
Then, the normalized minimum determinant of a lattice L in $M_n(\mathbb{C})$ may be defined as

$$\delta(L) = \min\det(L)/(\mathrm{vol}(L)^{n/k}).$$

The *shortest nonzero vector* of k-dimensional lattice L is denoted by $\mathsf{sv}(L)$.
The *normalized shortest vector* is then defined to be

$$\mathsf{Nsv}(k) = \sup\{\mathsf{sv}(L)/(\mathrm{vol}(L)^{1/k}) : L \text{ a } k\text{-dimensional lattice}\}.$$

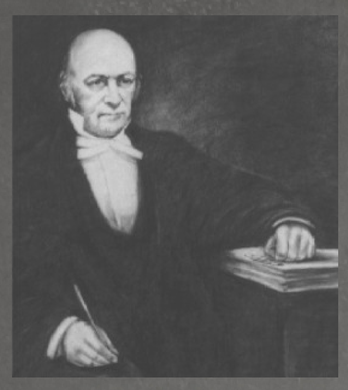
Example 1 : the Alamouti code

We consider the algebra $\mathcal{A} = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1)$. The lattice code $\psi(\Gamma_2)$ yields codewords of the form

$$\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, \text{ with } a, b \in \mathbb{Z}[i].$$

An interesting thing is that $\mathbb{R}(\psi(\Gamma_n)) = \mathbb{H}$, the Hamilton quaternion algebra.

Moreover the normalized minimum determinant is given by $\delta(\psi(\Gamma_2)) = 1/4$.



Example 2 : the Golden code

The Golden code is obtained by considering the algebra $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i)$. Let $\alpha = 1 + i(1 - \sqrt{5})/2$. Result 3 implies that $\psi(\Gamma_2\alpha)$ is a perfect code yielding codewords of the form

$$X = \begin{pmatrix} \alpha(a + b\nu) & i\overline{\alpha}(c + d\overline{\nu}) \\ \alpha(c + d\nu) & \overline{\alpha}(a + b\overline{\nu}) \end{pmatrix},$$

with $\nu = (1 + \sqrt{5})/2$ and $a, b, c, d \in \mathbb{Z}[i]$. Moreover, the normalized minimum determinant of the code is given by $\delta(\psi(\Gamma_2\alpha)) = 1/\sqrt{5}$.

Illustration : portrait of Sir W. R. Hamilton (1805-1865), Enterprise Ireland Portrait Gallery (http://www.maths.tcd.ie/pub/HistMath/People/Hamilton/).

Un grand merci à toutes les personnes qui ont déjà été remerciées au début du manuscrit de ce projet de master, dont vous venez de découvrir une partie du travail. Une mention spéciale va à Thomas Lugrin qui m'a soutenu et conseillé dans la dernière phase de l'élaboration de ce poster. Merci également à l'association CQFD pour l'organisation de l'édition 2012 du concours.

Codes from number fields

Let $E/\mathbb{Q}(i)$ be a Galois extension of degree n, with Galois group

$$\mathrm{Gal}(E/\mathbb{Q}(i)) = \{\sigma_1, \ldots, \sigma_n\}.$$

Let $\mathcal{O}_E$ denote the ring of integers of E. We consider the following *relative canonical embedding*

$$\begin{aligned} \psi : E &\longrightarrow M_n(E) \\ x &\longmapsto \begin{pmatrix} \sigma_1(x) & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \sigma_n(x) \end{pmatrix}. \end{aligned}$$

Result 1. Let $a \in E^\times$. Then $\psi(a\mathcal{O}_E)$ is a $2n$-dimensional lattice code in $M_n(\mathbb{C})$ with NVD property. Moreover

$$\delta(\psi(a\mathcal{O}_E)) = 2^{n/2}|d(E/\mathbb{Q})|^{-1/4},$$

where $d(E/\mathbb{Q})$ denotes the discriminant of E over $\mathbb{Q}$.

Codes from cyclic division algebras

Let $E/\mathbb{Q}(i)$ be a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/\mathbb{Q}(i)) = \langle\sigma\rangle$.
We call *cyclic* algebra and denote by $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ the $\mathbb{Q}(i)$-algebra defined by

$$\mathcal{A} = E \oplus uE \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations

$$xu = u\sigma(x) \text{ for all } x \in E \text{ and } u^n = \gamma \in \mathbb{Q}(i)^\times.$$

Denote by Γ_n the following subgroup of $\mathcal{A}$

$$\mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E.$$

We consider the following *relative canonical embedding*

$$\begin{aligned} \psi : \mathcal{A} &\longrightarrow M_n(E) \\ x_0 + ux_1 + \ldots + u^{n-1}x_{n-1} &\longmapsto \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & \ldots & \gamma\sigma^{n-1}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \end{aligned}$$

Result 2. Let $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ be a cyclic division algebra of degree n with $\gamma \in \mathbb{Q}(i)^\times$, and $a \in E^\times$. Then $\psi(\Gamma_n a)$ is a $2n^2$-dimensional lattice code in $M_n(\mathbb{C})$ with NVD property. Moreover

$$2^{n^2/2}|d(E/\mathbb{Q})|^{-n/4}|v(\gamma)|^{-n}|\gamma|^{-n(n-1)/2} \leq \delta(\psi(\Gamma_n a)) \leq \frac{\mathsf{Nsv}(2n)^n}{n^{n/2}}.$$

Furthermore if $\gamma \in \mathbb{Z}[i]$, $|\gamma| = 1$, we have

$$\delta(\psi(\Gamma_n a)) = 2^{n/2}|d(E/\mathbb{Q})|^{-1/4}.$$

Perfect codes

A lattice code $\mathcal{C} \subseteq M_n(\mathbb{C})$ is said to be *perfect* if it can be written in the form

$$\mathcal{C} = \mathbb{Z}[i]M_1 \oplus \cdots \oplus \mathbb{Z}[i]M_{n^2},$$

where $\{M_1, iM_1, \ldots, M_{n^2}, iM_{n^2}\}$ forms an orthonormal set with respect to the real Frobenius norm.

Result 3. Let $\mathcal{A} = (E/\mathbb{Q}(i), \sigma, \gamma)$ be a division algebra of degree n with $\gamma \in \mathbb{Z}[i], |\gamma| = 1$. If $\psi(a\mathcal{O}_E)$ is an orthonormal lattice code with $a \in E^\times$ then $\psi(\Gamma_n a)$ is a perfect code.

Mathematics institute of geometry and applications

Mathematics section

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE